REMARKS

Applicant appreciated the courtesy of a telephone conference with Examiner Pyzocha.

During the telephone conference, a brief discussion was conducted on the comments in the continuation sheet of the Advisory Action. More specifically, the *Colligan* (U.S. Patent No. 6,415,031) was mentioned as directed to a mode in which all the frames, including I-frames, P-frames, and B-frames in MPEG-2 can be encrypted, and another mode in which only I-frames are encrypted.

The Examiner indicated that he believed that the definition of a normal reproduction mode and a particular reproduction mode were in general too broad in the claims and accordingly, he reviewed the cited references in this light against the claims.

Applicant indicated that it intended to submit claims providing a new definition of a normal reproduction mode and a particular reproduction mode along with the manner in which the descrambling keys were used. Examiner Pyzocha indicated that such elements, if properly set forth in the claims, would assist in view of the art of record. Examiner Pyzocha did not make any commitment as to allowability, and reserved the right for further searching.

Examiner Pyzocha was also kind enough to indicate that when he receives the amended claims, that he was willing to have a further discussion, if any issues remained.

Claims 1-3, 11-12, 15, 17-19, 22-29 and 31-34 were rejected as being obvious over *Hirose* (U.S. Patent No. 5,917,915) in view of *Akiyama* (U.S. Patent No. 6,463,155) when taken further in view of the *Colligan* (U.S. Patent No. 6,415,031).

The present invention is directed to a broadcast apparatus such as pay subscription movies where scrambled video signals can be processed and descrambled by a reception apparatus, to allow a television viewer to save and view scrambled television programs in modes

other than a normal reproduction mode, e.g., a play mode at a play reproduction speed. Due to the manner in which the frames are scrambled, and the procedure in which a fast forward or rewind modes are implemented, the order and rate of reproduction of the individual frames is changed. The reception apparatus, accordingly, must find and retrieve a descrambling key from a previous video unit or set of frames, with a corresponding burden on the reception apparatus and a processing speed that can be accomplished. As a result, poor or no video reproduction can occur in such particular modes.

The present invention as defined in our current claims addresses these problems by providing a list of descrambling keys which includes all of the descrambling keys, each of which are required to decrypt each frame of the content. Using the list of descrambling keys, a reception apparatus of the present invention can retrieve a descrambling key efficiently even in a particular reproduction mode at a different reproduction speed than a normal reproduction speed of a normal playback. This is because, in our invention, the reception apparatus can retrieve the descrambling key from the list of the descrambling keys, and need not perform a burdensome operation of retrieving a descrambling key from a previous video unit or set of frames.

While the *Hirose* reference proposes double encrypting newspaper data with a first key and a second key to select subscribers. It does not recognize nor address the problems that can occur with video images, and particularly reproducing video images from scrambled video data that is broadcast and may be stored for later play.

The *Akiyama* reference is primarily concern with monitoring broadcast services that would be available to a subscriber using a master key that controls access to individual channel keys. A master key can encrypt a reception device ID as well as contract information for the reception device. A master key is used by the receiver to decrypt the contract information and to

obtain the individual channel keys. Again, there is no recognition of the problem nor solution offered as defined by our current claims.

The *Colligan* reference is relevant in addressing a video-on-demand distribution network wherein digital video signals are transmitted from a video server to each individual viewer who subscribes. *Colligan* was attempting to address the high cost that could occur with encrypting the requested digital video-on-demand in real time whenever requested by each individual viewer. Basically, *Colligan* teaches purportedly a higher security system that is disclosed in Figure 5A. A video-on-demand source generates an encrypted program to create a first encrypted form. This is transmitted via a primary distribution network from the video-on-demand source to a remote server. The encrypted program is stored at the remote server.

When the remote server receives a request for transmission of a video program from a subscriber station, the remote server decrypts the video program from the first encrypted form and a first key is used for this decryption. This first key can be received via a communication channel separate from the transmission channel of the video program. This decrypted video program is then re-encrypted with a second key. This second key, for example, can be a public key in a public key encryption system. As known, a public key encryption system can use two different keys, a public key to encrypt data and a private key to decrypt data.

The re-encrypted program is then multiplexed with other signals and broadcast to subscriber stations. The re-encrypted program is then de-multiplexed at appropriate subscriber stations. The re-encrypted program is then decrypted with the second key so it can be displayed on a television monitor connected to a set top box, for example in a home system or in a hotel room.

Compare this teaching, however, with the problem addressed by our present invention as can be seen on Page 3, Line 16 to Page 4, Line 1. As can be appreciated, this is a totally different problem than that addressed by *Colligan.*

In *Orthopedic Co., Inc. v. United States*, 217 USPQ 193 (C.A.F.C. 1983), the Federal Circuit set forth a useful guide for determining the scope and content of the prior art. Orthopedic, at pages 196-197, also focuses on the "problem" faced by the inventors:

> In determining the relevant art. . . one looks at the nature of the problem confronting the inventor.
>
> * * *
>
> [W]ould it then be <u>nonobvious</u> to this person of ordinary skill in the art to <u>coordinate these elements in the same manner as the claims</u> in suit? The difficulty which attaches to all honest attempts to answer this question can be attributed to the <u>strong temptation to rely on hindsight</u> while undertaking this evaluation. It is wrong to use the patent in suit [the patent application before the Examiner] as a guide through the maze of prior art references, combining the right references in the right way so as to achieve the result of the claims in suit. <u>Monday morning quarterbacking is quite improper when resolving the question of nonobviousness</u>. (Emphasis added)

More specifically, in the *Colligan* reference (a) the mode in which all frames are encrypted or (b) the mode in which only I-frames are encrypted, is selected based on the security level. In this case, a key used for encrypting all the frames should be different from a key that is used to encrypt only the I-frames, and there should be no corresponding relationship between the two types of keys.

In contrast, our amended independent reception apparatus claims differ from the *Colligan* reference in that only one content, namely a scrambled content that is generated by encrypting all frames, is used, and that in the normal reproduction mode in which a reproduction is performed by decrypting all the frames, all the frames are decrypted (descrambled), and in the particular

reproduction mode in which a reproduction is performed by decrypting part of the frames, only a selected number of the total frames are decrypted.

It is possible to receive a key list that includes all descrambling keys that correspond to all the frames, and extract necessary descrambling keys from the key list. This makes it possible to perform the process of extracting the descrambling keys in a short time and with a low level of processing loads. The keys used in the particular reproduction mode are a subset of the keys used in the normal reproduction mode. This produces an advantageous effect of increasing the performance level of the particular reproduction to a satisfactory level.

Our present claims now provide a definition of the normal reproduction mode and the particular reproduction mode for each of the reception apparatus claims. Additionally, our claims define each frame in the scrambled mode as being scrambled so that it can be decrypted using a descrambling key that corresponds to the frame and a descrambling key list, including all the descrambling keys as received. In a normal reproduction mode, all the descrambled keys are extracted and sequenced from this scrambled key list and all the frames are descrambled to reproduce the full content.

However, in a particular reproduction mode, e.g. fast forward or fast reverse mode, the only descrambling keys corresponding to predetermined frames to be reproduced are selected in accordance with this particular reproduction mode. These descrambling keys are selectively extracted and only the predetermined frames from all of the frames are descrambled to reproduce the content.

In summary, disregarding the broad teaching of *Colligan* for addressing unrelated problems, at most, the *Colligan* reference can be relied upon for a technology of switching

between (a) a mode in which all the frames, including I-frames, P-frames and B-frames in MPEG-2 are encrypted, and (b) a mode in which only I-frames are encrypted.

As a result of our amendment to the claims, it is respectfully submitted that the particular reproduction mode of our present invention cannot be held to correspond to a mode in which only I-frames are encrypted. Additionally, the *Colligan* reference does not include, nor recite, nor address the problems associated with a different reproduction speed in a fast forward or fast reverse mode. Thus, not only the concept of the present invention is lacking from the teachings of the *Colligan* reference, but it is unlikely that the *Colligan* reference would be combined with either the *Hirose* or *Akiyama* references to render obvious the presently amended claims under 35 U.S.C. §103.

If the Examiner believes that a telephone interview will help further the prosecution of this case, the undersigned attorney can be contacted at the listed telephone number.

Very truly yours,

SNELL & WILMER L.L.P.
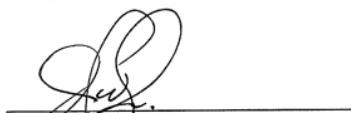
Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626-7689
Telephone: (714) 427-7420
Facsimile: (714) 427-7799